C-6-3-7

LGPKI

Application Certification Authority G3 (Root)

CP/CPS

Version 1.3

December 13, 2016

Japan Agency for Local Authority Information Systems

LGPKI Application Certification Authority G3 (Root) CP/CPS
Established by the Japan Agency for Local Authority Information Systems, January 26, 2015.
Revised on December 18, 2015
Revised on October 14, 2016
Revised on December 13, 2016

1 Introduction

This document (hereinafter referred to as "CP/CPS") lays down operating rules for the certification work performed by the LGPKI Application Certification Authority G3 (Root) (hereinafter referred to as "Application CA G3 (Root)"); the Application CA G3 (Root) is the root certification authority, which is placed at the highest hierarchical level above the subordinate certification authorities that issue certificates for web servers, etc. to local governments, those organizations authorized to be provided with LGWAN functions under the provisions of Paragraph 2 of Article 7 of the *Rules and Regulations for the Local Government Wide Area Network* (hereinafter referred to as "J-LIS authorized organizations"), and LGWAN-ASP services providers.

Application CA G3 (Root) shall comply with the guidelines stipulated in the latest publication of "AICPA/CICA, WebTrust Program for Certification Authorities" and "CA/Browser Forum, Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificate."

If any conflict arises between this CP/CPS and any of the requirements of these guidelines, the requirements of these guidelines shall take precedence over this CP/CPS.

In this CP/CPS, "local governments" refers to the local governments set forth in the *Local Autonomy Law* and which connect to the Local Government Wide Area Network (hereinafter referred to as "LGWAN"). Also, LGWAN-ASP service providers are those that provide the LGWAN-ASP services set forth in the *Rules and Regulations for the Local Government Wide Area Network*.

The composition of this CP/CPS is based on the RFC (Request For Comments) 3647 *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, issued by the IETF (Internet Engineering Task Force) PKIX (Public-Key Infrastructure X.509) Working Group.

For descriptions in this CP/CPS, the items specified in RFC3647 are utilized. However, when referring to other rules, only their headings are mentioned, and the contents to be referenced are specified.

1.1 Outline

1.1.1 Types of Certificates

Application CA G3 (Root) issues subordinate CA certificates to LGPKI Application Certification Authority G3 (Sub) (hereinafter referred to as “Application CA G3 (Sub)”). Application CA G3 (Root) also issues certificates of OCSP responder that is prepared for relying parties on the Internet side (hereinafter referred to as “OCSP responder certificate”) to the operation unit of Local Government Wide Area Network (hereinafter referred to as the “Operation Unit”).

1.1.2 Related Rules

Rules related to LGPKI and the Application CA G3 (Root) are as follows. In this CP/CPS, related rules are referred to as necessary.

- Local Government Wide Area Network Basic Outline
- Basic Framework for Operation of Local Public Organization Certificate Infrastructure
- Local Government Wide Area Network ASP Basic Framework
- LGPKI Application Certification Authority G3 (Sub) CP/CPS

1.2 Document Name and Identification

Certificate policies of the Application CA G3 (Root) have the following identifiers.

- Subordinate CA certificates - policy: [1.2.392.200110.10.8.5.1.101.10]

1.3 PKI-related Parties

1.3.1 Operational Organizations

Figure 1-1 illustrates the organizations that constitute and relate to the Application CA G3 (Root) and their relationship.

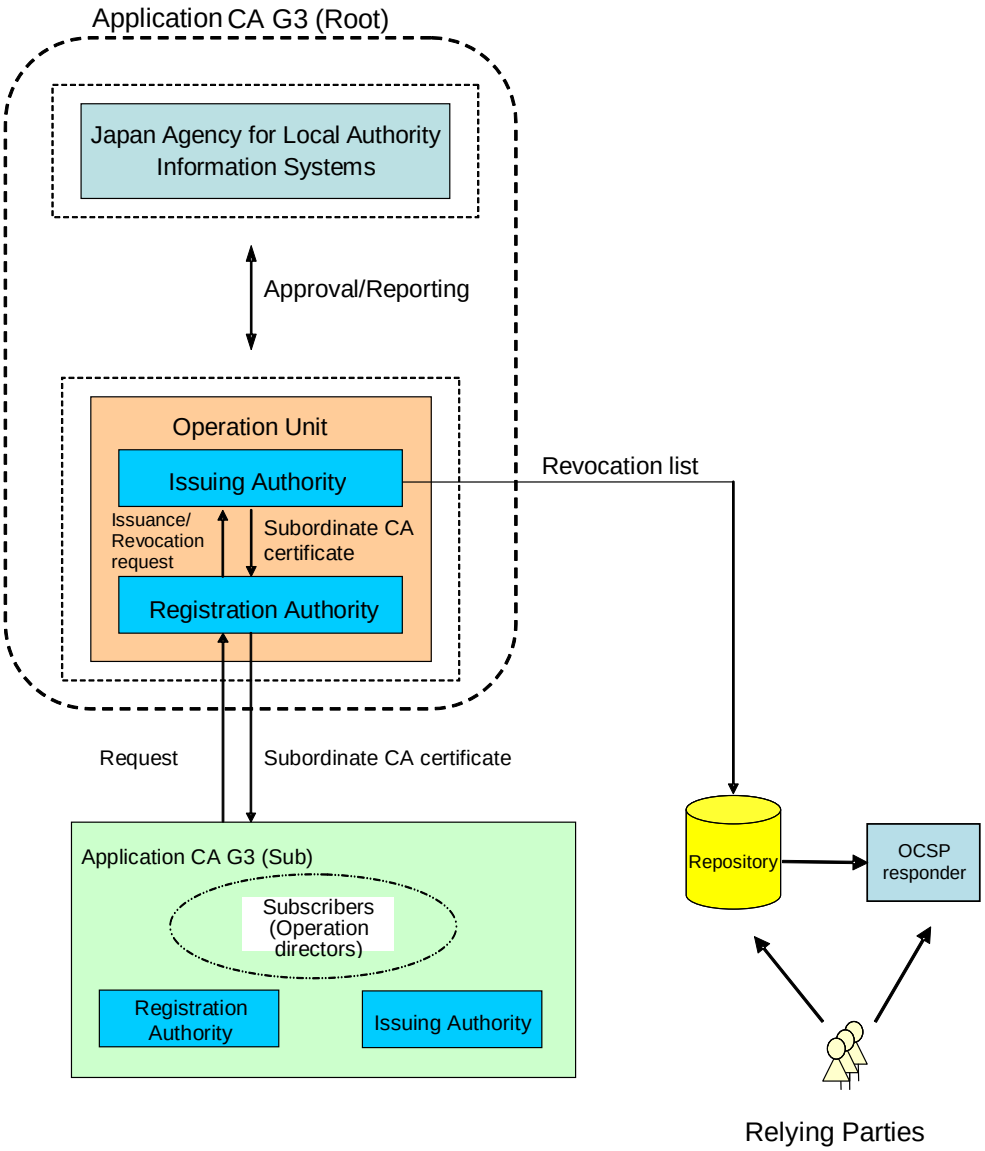

Figure 1-1 Organizations and their Relationship

The organizations and their roles are listed in Table 1-1.

Table 1-1 Organization Units and Roles

Organization Unit	Roles
Japan Agency for Local Authority Information Systems	As the decision-making organization for operation of the Application CA G3 (Root), decides the following matters. ・Establishment and revision of CP/CPS for the Application CA G3 (Root) ・Response when CA private keys are compromised ・Emergency response during disasters, etc. ・Other important matters concerning operation of the Application CA G3 (Root)
Operation Unit	As the operating organization for the Application CA G3 (Root), mainly performs the following work. ・Reporting on operating status to the Japan Agency for Local Authority Information Systems ・Operation of the Application CA G3 (Root) ・Operation and maintenance of CA system (Registration Authority) ・Reception and examination of requests for issuance, renewal, and revocation of subordinate CA certificates ・Making of requests for issuance and revocation of subordinate CA certificates (Issuing Authority) ・Issuance and revocation of subordinate CA certificates As the operation organization, the following Certification Authority operating staff shall be allocated. Certification Authority Chief, Certification Authority system Chief, Keys Manager, Receptionist, Examiner, Examination Approver, IA Operator, RA Operator, Repository Operator, VA Operator and Audit Log Investigator.
Subscribers	Subscribers in this CP/CPS are the operation directors of the Application CA G3 (Sub). They manage the certificates issued by the Application CA G3 (Root), and use those certificates in accordance with this CP/CPS.
Relying Parties	Relying parties check the validity of certificates, by referring to a list providing information on the revocation of subordinate CA certificates (hereinafter referred to as “CRL”) or the OCSP responder.

1.3.2 Other Related Parties

Not specified.

1.4 Uses of Certificates

The Application CA G3 (Root) is a CA that functions at the highest hierarchical level above subordinate CAs, and which issues subordinate CA certificates to the Application CA G3 (Sub). Relying parties, which use certificates with confidence, may verify the reliability of applicable certificates by using self-signed certificates for the Application CA G3 (Root).

1.5 Policy Management

1.5.1 Organizations Responsible for Managing Documents

Work related to changing, renewing, and the like for this CP/CPS shall be conducted by the Japan Agency for Local Authority Network Systems (hereinafter referred to as “J-LIS”).

1.5.2 Contact

The Operation Unit is the contact point for inquiries regarding this CP/CPS. The contact point is shown on the following web page.

URL of public web server: http://www.lgpki.jp/

URL of web server for local governments: http://center.lgwan.jp/use/third2_5.html

1.5.3 Party Responsible for Determining Policy Conformity

The conformity of the Application CA G3 (Root) shall be determined by the J-LIS.

1.5.4 Approval Procedure

The validity of the CP/CPS of the Application CA G3 (Root) shall be determined by the J-LIS.

1.6 Definitions and Abbreviations

・CA (Certification Authority)

Issues and revokes public key certificates for owners of key pairs (private key and public key). In the LGPKI, the bridge CA, organization CA, and Application CA all mean the same thing, comprised of an Issuing Authority and Registration Authority.

・CAA (Certification Authority Authorization)

In relation to the authorization to use domains, it is a function to describe in the DNS record Certification Authority information that allows issuing a certificate to a domain for the purpose of preventing unintended issue of a certificate by the Certification Authority from being made by mistake.

・CA System

System which comprises the Certification Authority. In the LGPKI, this signifies the IA system, HSM, RA system, and repositories.

・CP (Certificate Policy)

Policy applying to certificates for specific a community or application, accompanying general security requirements.

- CPS (Certification Practice Statement)

  Certification Authority operation rules. Execution procedures in order to apply policies specified in the CP for operation of the Certification Authority. This document provides detailed specifications for legal stipulations, reliance on external parties, etc.

- CRL (Certificate Revocation List)

  List identifying certificates which were revoked before their expiration date. Usually, it is digitally signed by the CA.

- FIPS (Federal Information Processing Standardization)

  FIPS140-2 is a criteria for encryption module evaluation.

- HSM (Hardware Security Module)

  An HSM is a private key management device with tamper resistant functions. It stores CA private keys.

- IA (Issuing Authority)

  As part of CA operations, issues and revokes certificates.

- IA System

  Issuing Authority system. System which issues and revokes certificates.

- OCSP (Online Certificate Status Protocol)

  Name of the protocol for on-line checking of the validity of applicable certifications.

  The server that verifies the validity of the certificates designated by relying parties and returns the verification results of the certificates to the relying parties is called “OCSP responder.”

  Application CA G3 (Root) provides the OCSP responder conforming to RFC2560 and RFC5019.

- PIN (Personal Identification Number)

  In the LGPKI, this signifies a password used in CA private key activation, a password used in activation of an IC card distributed to a subscriber, a password used to setup the private key protection when a subscriber generates a key pair, etc.

- PKI (Public Key Infrastructure)

  Infrastructure for strict (certain) personal authentication (personal confirmation) via the Internet.

- PKCS (Public Key Cryptography Standards)

  Industry standards advocated by RSA Laboratories USA. This group of industry standards aims at portability of applications surrounding encryption operations such as encryption algorithms, and mutual connectivity.

  PKCS#1: RSA Cryptography Standard. Specifies signature format, etc.

  PKCS#7: Cryptographic Message Syntax Standard

  PKCS#10: Certification Request Standard

  PKCS#12: Personal Confidential Information Standard

・RA (Registration Authority)

Registration authority. The RA conducts registration work, which is part of the work of a CA. In the LGPKI, it signifies the Registration Authority placed in the Operation Unit, or the Registration Authority Branch placed in a local government or a J-LIS authorized organization to which part of registration work is delegated.

・RA System

Registration Authority system. This system enables processing of requests related to certificate issuance and revocation. The RA system is able to manage the flow of a series of processes, from receiving data on requests from subscribers, through examination, approval, and issuance.

・RFC (Request For Comments)

Series of document groups which the IETF brings together.

・RSA (Rivest-Shamir-Adleman)

Currently the most popular public key encryption method. The difficulty of doing factor analysis of number from two sufficiently large prime numbers multiplied together is a foundation of encryption technology.

・SHA-1 (Secure Hash Algorithm-1)

One-way hash algorithm which generates a 160bit hash value from data of various lengths.

・SSL (Secure Sockets Layer)

Protocol which encrypts and authenticates communications between server and client, securely exchanging data.

・VA (Validation Authority)

In response to a certificate validity confirmation inquiry from a relying party, the VA replies after verifying the electronic signature of that certificate, and checking its expiration date and revocation information.

・X.500

X.500 was established by the ITU-T (Telecommunication Standardization Sector of the International Telecommunications Union). It is an international standard concerning distributed directory services in the network. X.500 establishes a directory concept, directory hierarchical structure, definitions of services and objects, etc.

・X.509

X.509 is a recommendation of ITU-T (Telecommunication Standardization Sector of the International Telecommunications Union). It provides a technical standard concerning authentication from technology of the directory field. This specifies the roles of a Certification Authority (CA), public key certificates, revocation lists, attributes used, etc.

・Archive Data

Electronic data which gathers certificates, CRL, operations history, etc.

・Access Log

Electronic data which recorded identification information for system access: date, time, actions, access source, etc.

- Object Identifier (OID)

  Identifier allocated which is unrelated to the information's meaning, in order to mutually differentiate information. OIDs are managed by a tree structure, in order to specify uniquely.

- Subordinate CA Certificate

  A public key certificate issued by the Application CA G3 (Root) to certify that a subordinate CA is reliable.

- Key Storage Media

  Media which stores public key certificates, private keys, etc. In the LGPKI, this signifies IC cards, USB tokens, and HSM which store subscriber public key certificates and private keys, etc.

- Activation

  Change the status of a private key to enable its use.

- Audit Log

  Electronic data which recorded security related events: type, date, time, operator identification information, etc.

- Compromise

  To become compromised. In the LGPKI, this signifies a situation where it is judged that the private key of a CA or subscriber passed into the hands of a third party due to being lost/stolen/etc. (or if it is highly probable), or where the possibility has been identified that a private key can be easily calculated from the public key.

- Public Key Certificate (Certificate)

  After the CA checks the certificate content, the CA signs it electronically, thereby guaranteeing that public key's validity.

- Public Key

  Disclosed key which is one side of the key pair used in a public key encryption method, corresponding to the private key.

- Self-Signed Certificate

  Certificate which was electronically signed by the CA's own private key, corresponding to the CA's own public key. This guarantees the validity of the CA's own public key.

- Revocation

  Invalidation of a certificate before the certificate expiration date, due to a reason such as its private key is compromised, change in information noted in the certificate, or the certificate's use is terminated.

- Relying Party

  Party which receives a certificate, and relies on it when acting.

- Subscriber

  A private key holder who is a user of a public key certificate. A subscriber can be an individual, or it can also be a server application, etc. In the LGPKI, this signifies a certificate holder which belongs to a local government, an organization authorized by the council, or a LGWAN-ASP service provider.

・Digital Signature

Hash value of data to be signed, which is encrypted by a private key. A digital signature can be verified by comparing the value of the digital signature decrypted by the public key, against the original data's hash value. A digital signature can only be generated by that private key holder, thus it is assumed to have the same effect as a handwritten signature.

・Electronic Signature

Signature which is attached in order to identify the creator of an electronic document, and confirm that the electronic data was not changed. Indicates electronic signature actions in general, including digital signatures.

・Certification Path

Chain of certificates required in order to validate one certificate.

・Hash

Algorithm in order to compress data of varying length into fixed length data. It is impossible to reproduce the original data from its hash value. A one-way hash algorithm is used as a checksum to confirm that the message is neither damaged nor falsified, and is used in digital signatures.

・Private Key

A key held only by the owner, which is one side of a key pair used in a public key encryption method, corresponding to the public key.

・Repository

Holds information concerning various objects, and provides a procedure to search and renew that information. Its international standards specifications are the ITU-T Recommendation X.500 series, and the ISO/IEC international standard 9594 series (OSI directory).

It stores and discloses: self-signed certificates, link certificates, and CRL. The LGPKI repository is comprised of an integration repository and public repository, with the integration repository disclosed via the LGWAN, and the public repository disclosed via the Internet.

・Link Certificate

Certificate to guarantee the relationship between a new CA key pair and old CA key pair.

2 Announcement and Duties of Repository

2.1 Repository

The repository has the following duties.

- Announce information specified in *2.2 Announcement of Information on Certificates* in this CP/CPS.
- Part of the information registered in the integrated repository shall be duplicated in the public repository.
- In principle, provide stable 24/365 operation.
- Protect registered information.
- During the operation hours specified above, make responses to legitimate requests for information search.

However, operations may be temporarily suspended due to maintenance, etc. Also, the repository does not guarantee that an announced CRL incorporates the latest valid information that may be obtained at the moment a relying party performs verification.

2.2 Announcement of Information on Certificates

Information concerning the Application CA G3 (Root) shall be announced via the integrated repository, public repository, web server and OCSP responder. These web servers include a web server provided to local governments via the LGWAN (hereinafter referred to as "web server for local governments"), a web server provided to local governments and LGWAN-ASP service providers etc. via the LGWAN (hereinafter referred to as "web server for LGWAN-ASP services"), and a public web server provided to residents and companies etc. via the Internet (hereinafter referred to as "public web server"). OCSP responder is provided to relying parties via the Internet.

(1) Announcements via repositories

(Integrated repository)

- A self-signed certificate, a subordinate CA certificate, and a CRL that are issued by the Application CA G3 (Root).

  Details shall be provided in the technical specifications announced on the web server for local governments.

(Public repository)

- A self-signed certificate, a subordinate CA certificate, and a CRL that are issued by the Application CA G3 (Root).

  Details shall be provided in the technical specifications announced on the public Web server.

(2) Announcements via web servers

(Web server for local governments)

- Information on CA private key compromise
- Application CA G3 (Root) CP/CPS
- Revision history of the Application CA G3 (Root) CP/CPS
- Self-signed certificates of the Application CA G3 (Root)

- Fingerprints of Application CA G3 (Root) self-signed certificates
- LGPKI Subscriber Handbook (version for local governments)
- Profile design
- Technical specifications

(Web server for LGWAN-ASP service providers)

- CRL of the Application CA G3 (Root)
- LGPKI Subscriber Handbook (version for LGWAN-ASP service providers)

(Public web server)

- Information on CA private key compromise
- Application CA G3 (Root) CP/CPS
- Revision history of the Application CA G3 (Root) CP/CPS
- Self-signed certificates of the Application CA G3 (Root)
- CRL of the Application CA G3 (Root)
- Fingerprints of Application CA G3 (Root) self-signed certificates
- LGPKI Subscriber Handbook (version for LGWAN-ASP service providers)
- Profile design
- Technical specifications

(3) Announcements via OCSP responder

OCSP responder is provided so that relying parties can perform on-line confirmation of the validity of certificates.

2.3 Timing and Frequency of Announcements

The renewal frequency of information announced is as follows.

- Each certificate and its CRL that are specified in *2.2 Announcement of Information on Certificates* of this CP/CPS shall be announced each time they are issued or renewed.
- Each time there is a change in CP/CPS
- LGPKI Subscriber Handbook (version for local governments), LGPKI Subscriber Handbook (version for LGWAN-ASP service providers), profile design, and technical specifications shall be announced each time a change is made.

2.4 Control of Access to Repository

Information announced via the public repository, public web server or OCSP responder shall be provided via the Internet. In providing this announced information, special access controls shall not be applied. Information announced via the web server for local governments shall be provided via LGWAN, only to local governments. Information announced via the integrated repository and web server for LGWAN-ASP, shall be provided via LGWAN to local governments, LGWAN-ASP service providers, etc.

3 Identification and Certification

3.1 Determination of Names

3.1.1 Types of Names

The issuer name and main party name of a subordinate CA certificate shall be given according to the X.500 Distinguished Name (DN) format.

3.1.2 Necessity for the Meanings of Names

The names used in subordinate CA certificates shall be that specified by the subscriber, and the Certification Authority name specified by the Application CA G3 (Root).

3.1.3 Anonymity and Pseudonymity of Subscribers

This shall be as stated in *3.1.2 Necessity for the Meanings of Names* of this CP/CPS.

3.1.4 Rules for Interpreting Name Formats

The rules applied to the interpreting of the formats of names shall be in line with the rules and the like set forth by the Application CA G3 (Root).

3.1.5 Uniqueness of Names

The main party names of the certificates issued by the Application CA G3 (Root) shall be allocated uniquely.

3.1.6 Roles of Recognition, Certification, and Registered Trademarks

If there is a dispute concerning names, the Application CA G3 (Root) shall have the authority to make the ultimate decision.

Restrictions, handling, and disputes concerning registered trademarks are as follows.

- Subscribers shall not make requests which would infringe on another party's registered trademark.
- The Application CA G3 (Root) does not verify whether a registered trademark belongs to a subscriber.
- The Application CA G3 (Root) does not provide arbitration nor mediation etc. for disputes concerning ownership of registered trademarks.
- The Application CA G3 (Root) is able to reject requests, using dispute concerning ownership of a registered trademark as a reason.

3.2 First Identification and Certification

3.2.1 Method for Verifying the Possession of Private Keys

When a subscriber generates a key pair, verify the electronic signature of the certificate issuance request to ensure that it is electronically signed using the private key corresponding to the included public key.

3.2.2 Certification of Organizations

In the process of responding to a request for a subordinate CA certificate, the Registration Authority shall follow prescribed procedures to confirm the existence and identity of the organization to which the subscriber belongs.

3.2.3 Certification of Individuals

The Application CA G3 (Root) shall not issue certificates for individuals.

3.2.4 Unverified Information on Subscribers

Not specified.

3.2.5 Verification of Legitimacy of Authority

The legitimacy of authority shall be verified according to the procedures specified in *3.2.2 Certification of Organizations* of this CP/CPS.

3.2.6 Standard for Mutual Operation

Not specified.

3.3 Identification and Certification for Renewal Request

3.3.1 Identification and Certification for Normal Renewal

Identification and certification for the renewal of certificates shall be performed according to the procedures specified in *3.2 First Identification and Certification* of this CP/CPS.

3.3.2 Identification and Certification for Renewal of Certificates after Their Revocation

Identification and certification for the reissuance of a certificate after its revocation shall be performed according to the procedures specified in *3.2 First Identification and Certification* of this CP/CPS.

3.4 Identification and Certification for Revocation Request

Identification and certification for the revocation of a certificate shall be performed according to the procedures specified in *3.2.2 Certification of Organizations* of this CP/CPS.

4 Operational Requirements for Lifecycle of Certificates

4.1 Request for Certificates

4.1.1 Certificate Applicant

Requests for subordinate CA certificates shall be made by the operation directors of the Application CA G3 (Sub).

4.1.2 Registration Procedure and Responsibilities

Requests for subordinate CA certificates shall be made by the operation directors of the Application CA G3 (Sub), and applicable operation directors shall provide accurate information.

4.2 Certificate Request Procedure

The Application CA G3 (Root) shall follow the procedures specified in *3.2.1 Method for Verifying the Possession of Private Keys* and *3.2.2 Certification of Organizations* of this CP/CPS to ensure that the details of requests are appropriate. Confirmation in reference to CAA record is not performed.

4.3 Issuance of Certificates

The Application CA G3 (Root) shall add its CA's electronic signature, and shall issue subordinate CA certificates.

4.4 Acceptance of Certificates

A subscriber shall immediately check the details of its subordinate CA certificate, and if there is an error in the description of the subordinate CA certificate, the subscriber shall make a request for revocation and issuance for the reason of the error.

Upon receiving no request from the subscriber, the Application CA G3 (Root) shall consider that the subordinate CA certificate has been accepted.

4.5 Use of Key Pairs and Certificates

4.5.1 Use of Private Keys and Certificates by Subscribers

Subscribers shall have the following responsibilities.

- Follow this CP/CPS when using subordinate CA certificates.
- Do not use subordinate CA certificates for uses other than those specified in 1.4 Uses of Certificates of this CP/CPS.
- Have responsibility for private keys for issued subordinate CA certificates.

4.5.2 Use of Public keys and Certificates by Relying Parties

Relying parties shall have the following responsibilities.

- Create and verify certification paths.
- Verify certificates used only for the uses specified in 1.4 Uses of Certificates of this CP/CPS.

4.6 Renewal of Certificates

When renewing a subordinate CA certificate, the procedures specified in *4.2 Certificate Request Procedure* and *4.3 Issuance of Certificates* of this CP/CPS shall be followed.

4.7 Renewal of Certificates in Association with That of Keys

Not specified.

4.8 Changes in Certificates

If there is a change in information on a subordinate CA certificate, another subordinate CA certificate shall be issued according to the same procedures as those specified in *4.2 Certificate Request Procedure* and *4.3 Issuance of Certificates* of this CP/CPS. Revocation of the already issued subordinate CA certificate in association with the change shall be done in the same way as specified in *4.9.3 Revocation Request Procedure* of this CP/CPS.

4.9 Revocation and Temporary Suspension of Certificates

4.9.1 Reasons for Revocation of Certificates

A certificate shall be revoked if any of the following occurs.

- Compromise of the applicable CA private key
- Compromise of the private key of the subscriber
- Change in the description of the certificate
- Cessation of the use of the certificate
- The J-LIS has concluded that the certificate needs to be revoked because of, for example, a breach of the obligations specified in this CP/CPS by the subscriber.
- The Certification Authority System Chief has concluded that the certificate needs to be revoked because, for example, the certificate was issued improperly due to a reason attributable to the Application CA G3 (Root).

Note that the revocation of an issued certificate shall not be cancelled. If a subordinate CA certificate is to be reissued for a subscriber for whom a subordinate CA certificate was revoked, issuance procedures shall be followed again.

4.9.2 Certificate Revocation Applicant

Requests for the revocation of subordinate CA certificates shall be made by subscribers. However, if the Certification Authority System Chief or the J-LIS considers that a subordinate CA certificate needs to be revoked, it shall be revoked under the instruction of the Certification Authority System Chief.

4.9.3 Revocation Request Procedure

Subscribers shall submit a written request for the revocation of a subordinate CA certificate to the Receptionist of the Registration Authority according to prescribed procedures.

The Application CA G3 (Root) shall revoke the certificate in question according to prescribed procedures, and shall register a CRL in both the repository and the web server. The Receptionist of the Registration Authority shall notify the subscriber of the revocation of a subordinate CA certificate.

Requests for revocation in the event of a disaster shall be made according to separately specified procedures.

4.9.4 Revocation Grace Period

The Application CA G3 (Root) shall perform revocation within two (2) business days after receiving the revocation request, provided that in the case of an urgent revocation request, it shall perform revocation immediately upon receipt thereof. The issuance of a CRL after the completion of the revocation is specified in *4.9.7 CRL Issuance Frequency* of this CP/CPS.

4.9.5 Period within which the Certification Authority Shall Deal with Revocation Requests

The Application CA G3 (Root) shall perform revocation within two (2) business days after receiving the revocation request, provided that in the case of an urgent revocation request, it shall perform revocation immediately upon receipt thereof.

4.9.6 Request for Revocation Investigation

Relying parties of subordinate CA certificates must check the validity of subordinate CA certificates. To enable their validity checking, the Application CA G3 (Root) shall issue CRLs on the repository and the web server, and also provide OCSP responder.

4.9.7 CRL Issuance Frequency

A CRL with a validity period of 90 days shall be issued every 89 days during normal operation. However, if a problem such the compromise of a CA private key occurs, a CRL shall be immediately issued.

4.9.8 Maximum Delay in Issuance of CRLs

After issuing a CRL, the Application CA G3 (Root) shall immediately incorporate it into the integrated repository.

4.9.9 Availability of Online Revocation and Status Check

Online validity verification shall be provided by CRLs announced on the repository and the web server, and by the OCSP responder.

4.9.10 Requirements for Online Revocation/Status Check

Online validity verification must be performed according to the CRL that is announced on the repository and the web server and is issued by the Application CA G3 (Root), or according to the verification results of certificates provided by the OCSP responder.

4.9.11 Other Formats for Available Revocation Information

Not specified.

4.9.12 Special Requirements to Prevent the Compromise of Keys

Not specified.

4.9.13 Reasons for Temporary Suspension of Certificates

A subordinate CA certificate shall not be temporarily suspended.

4.9.14 Applicant for Temporary Suspension of Certificates

Not specified.

4.9.15 Request Procedure for Temporary Suspension of Certificates

Not specified.

4.9.16 Period within which Temporary Suspension of Certificates May Continue

Not specified.

4.10 Services for Checking the Status of Certificates

4.10.1 Operational Feature

A service of checking the status of certificates according to CRLs and the OCSP responder is provided.

4.10.2 Availability of Service

In principle, integrated repository, public repository, web server and OCSP responder shall be in service for 24 hours and 365 days through stable operation. However, they are subject to a temporary interruption of service for maintenance or other reasons.

4.10.3 Optional Specifications

Not specified.

4.11 Termination of Registration

Not specified.

4.12 Deposit and Recovery of Private Keys

The deposit of private keys shall not be performed.

5 Management Relating to Facilities, Operation, and Implementation

5.1 Physical Management

5.1.1 Location and Structure

The Application CA G3 (Root)'s facility shall be located in a place not easily subject to damage from water, earthquake, fire, or other disaster, and its building structure shall be earthquake resistant and fire resistant, with measures taken to protect against intrusion. Also, equipment etc. used shall be installed in a secure location protected against disasters and intrusion.

5.1.2 Physical Access

Physical access controls with multiple security levels shall be implemented, corresponding to the importance of the certification work being done. The Application CA G3 (Root)'s facility shall perform authentication by IC cards and biometric authentication equipment which can identify people with operation authorization. Physical access authority shall be granted by a separately determined person responsible for the certificate infrastructure equipment room entry/exit control, taking into consideration the duty of each staff member specified in *5.2 Procedural Management* of this CP/CPS. The main site's facility shall be monitored 24/365 by monitoring staff and a monitoring system.

5.1.3 Electrical Power and Air Conditioning

The Application CA G3 (Root) shall secure sufficient power supply capacity for operation of its equipment etc., and shall take measures to prepare for power flickers, electricity outages, and voltage/frequency fluctuations. In situations when commercial electricity source is not supplied, electric supply will switch over to a generator within a certain time period. Also, air conditioning equipment shall be installed in order to properly maintain the equipment operating environment and the work environment of the Certification Authority operation staff.

5.1.4 Measures against Water Damage

In the building where the Application CA G3 (Root)'s equipment is installed, water leak detection devices shall be installed, and waterproofing measures shall be taken in the ceilings and floors.

5.1.5 Fire Prevention and Fire Resistance

The building in which the Application CA G3 (Root)'s equipment is installed shall be a fire resistant structure, and the room shall be built in a fire prevention section. Also, automatic fire alarm equipment and firefighting equipment shall be properly installed.

5.1.6 Media Storage

Media which contains archive data and backup data shall be stored in a lockable storage cabinet installed a room where proper entry/exit controls are performed, with proper controls on check-in/check-out of objects based on prescribed procedures.

5.1.7 Waste Disposal

Disposal of documents and storage media which contain information to be handled confidentially shall be by proper waste disposal based on prescribed procedures.

5.1.8 Off Site Backup

For off site storage of media with important data etc., transport route security shall be ensured, and the media storage facility shall have proper security measures implemented.

5.1.9 Earthquake

The building in which the Application CA G3 (Root)'s equipment is installed shall be an earthquake resistant structure, and measures shall be taken to prevent falling of equipment and fixtures.

5.2 Procedural Management

5.2.1 Reliable Roles

The work of each staff shall be as follows.

(Application CA G3 (Root))

(1) Certification Authority Chief

The Certification Authority Chief is responsible for operations of the Application CA G3 (Root), and performs the following work.

- Creation of Application CA G3 (Root)'s operation policies
- Management of response when a CA private key is compromised, and during disasters or other emergencies
- Approval of revisions to internal rules concerning Application CA G3 (Root) work procedures
- Appointment and dismissal of Certification Authority operation staff
- Creation of training plans for Certification Authority operation staff, and management of training execution reports

(2) Certification Authority System Chief

The Certification Authority System Chief is responsible for operations of certification work and the CA system, and performs the following work. More than one Certification Authority System Chief shall be appointed and in the event of an accident occurred to one Certification Authority System Chief, other Certification Authority System Chief(s) shall be responsible for the works.

- Management of certification work
- Work instructions to Certification Authority operation staff, and checking of work results
- Other management concerning Application CA G3 (Root) operations
- Manage storage of the PIN for the key (hereinafter referred to as "Control Key") which controls functions of the Hardware Security Module (HSM)
- Requests to grant or remove entry/exit authority to the separately determined person responsible for certificate infrastructure equipment room entry/exit control accompanying appointment or dismissal of Certification Authority operation staff

(3) Keys Manager

The Keys Manager is responsible for work which uses CA private keys, and performs the following work.

- Multiple Keys Managers perform the work.
- Activation of CA private keys
- Manage storage of Control Keys and backup media for CA private keys
- Operation of HSM during CA private key generation and self-signed certificate issuance
- Operation of HSM during renewal of CA private keys
- Operation of HSM and setting of CA private key backup media during backup of CA private key and during restore from backup

(4) Receptionist

The Receptionist receives requests for the issuance, renewal, and revocation of subordinate CA certificates, ensures coordination with subscribers, and manages request forms and the like.

(5) Examiner

The Examiner examines requests for the issuance, renewal, and revocation of subordinate CA certificates.

(6) Examination Approver

The Examination Approver approves the results of the Examiner's examination of requests for the issuance, renewal, and revocation of subordinate CA certificates.

(7) IA Operator

The IA Operator performs the following work concerning CA system settings management. Multiple IA Operators perform this work.

- Deactivation of CA private keys
- Launch and halt of the CA system
- Settings management concerning operation of the CA system
- Settings management concerning the CA system's database backup, and operations for backup, restore, and archive
- Establishment, registration, and changes of certificate policy
- Issuance, renewal, and revocation processes for self-signed certificates
- Issuance to staff, renewal, and revocation processes for system operation certificates

(8) RA Operator

The RA Operator issues, renews, and revokes subordinate CA certificates. This work shall be done by multiple RA Operators.

(9) Repository Operator

The Repository Operator performs work concerning settings management of the integration repository and public repository.

(10) VA Operator

VA Operator performs work concerning settings for certificates on the OCSP responder system.

(11) Audit Log Investigator

The Audit Log Investigator performs the following work concerning logs of the IA system.

- Investigation of audit logs
- Deletion of unnecessary audit logs

5.2.2 Number of Staff for Each Operation

For execution of important work such as issuance, renewal, and revocation of certificates, staff work authority will be separately allocated to create mutual checks. Multiple Keys Manager who performs CA private key operations shall be appointed.

5.2.3 Identification and Authorization of Each Role

Work instructions to each staff shall be given by the Certification Authority System Chief. When each staff person performs a CA system operation, the system shall identify and authenticate that the operator is a properly authorized person.

5.2.4 Roles to Be Divided by Duty

Not specified.

5.3 Human Resource Management

5.3.1 Career, Qualifications, Experience, and Reliability Requirements

There shall be the following Certification Authority operation staff.

- Officers of the Operation Unit
- Contracted staff
- Dispatched workers, based on the Law Concerning Securing the Proper Operation of Worker Dispatching Undertakings and Improved Working Conditions for Dispatched Workers

5.3.2 Career Investigation Procedure

The Operation Unit shall confirm identification of staff with certificate of enrolment or other document and check the careers and reliability of staff, based on prescribed procedures.

5.3.3 Training Requirements

When appointed, Certification Authority operation staff must receive the training required to execute their work. In addition, Certification Authority operation staff must take the examination with regard to the WebTrust standards and the BaseLine requirements in order to maintain the skills necessary to execute their work.

5.3.4 Retraining Time Periods and Requirements

If the work of Certification Authority operation staff changes, they must receive training for their new work.

5.3.5 Time Period and Sequence of Officer Changes

Not specified.

5.3.6 Penalties for Actions which Are Not Permitted

If Certification Authority operation staff commit an act which is not permitted, they may receive penalties as determined in employment rules or contract, etc.

5.3.7 Staff Contract Requirements

If the Operation Unit contracts out part of the Certification Authority operation work, it shall conclude a proper contract with the contractor which includes duty of confidential retention regarding the contracted work.

5.3.8 Documents Presented to Staff

The Operation Unit shall disclose to Certification Authority operation staff the required documents corresponding to their appointed roles.

5.4 Audit Logging Procedure

The Audit Log Investigator shall compare the log recording events occurring regarding the Application CA G3 (Root) (hereinafter referred to as “audit log”) with the work execution records, etc., and perform security audits to check improper operations or other unusual events.

5.4.1 Recorded Events

Audit logs such as an access log and operation log shall be recorded for important events concerning security for the Application CA G3 (Root). The audit log shall include the following information.

- Type of event
- Date and time the event occurred
- Result of each process
- Information identifying the event source (operator name, system name, etc.)

5.4.2 Audit Frequency of Audit Logs

In principle, the Audit Log Investigator shall perform weekly comparisons of the audit log with work execution records, etc. However, if approved by the Certification Authority system Chief, the audit log investigation period can be changed.

5.4.3 Audit Log Storage Period

Storage shall be for 7 years.

5.4.4 Protection of Audit Logs

The audit log shall enable execution of falsification prevention measures, and falsification detection.

The audit log backup shall be stored weekly in external storage media, and stored in a lockable storage cabinet installed a room where proper entry/exit controls are performed.

Audit log examination and deletion shall be performed by the Audit Log Investigator.

5.4.5 Audit Log Backup Procedure

The audit log shall be backed up daily, and stored weekly in external storage media.

5.4.6 Audit Log System

The audit log gathering function is one function of the IA system, and important events concerning security shall be gathered as audit log starting from the system launch time.

5.4.7 Notification of Record Events

Investigation of the audit log shall be done without notifying the people who generated the events.

5.4.8 Verification of Fragility

By investigating the audit log, security fragility of operation aspects and technical aspects of the IA system shall be evaluated.

5.5 Archive

5.5.1 Types of Archive Data

There shall be the following archive data.

- Issued certificates and certificate requests
- CRL issuance history
- History of IA system launches and halts
- Operation history of IA system

5.5.2 Storage Period of Archive Data

Archive data shall be retained for 10 years after the expiry date of the validity period of the applicable certificate.

5.5.3 Protection of Archive Data

For archive data, access controls shall be implemented, and measures taken to enable falsification detection. Backups of archive data shall be stored monthly in external storage media, and stored in a lockable storage cabinet installed a room where proper entry/exit controls are performed.

5.5.4 Archive Data Backup Procedure

Archive data shall be backed up daily, and stored monthly in external storage media.

5.5.5 Record Time Stamp Requirement

Time stamps shall be given to each record in archive data.

5.5.6 Archive Data Collection System

Not specified.

5.5.7 Archive Data Verification Procedure

External storage media in which archive data is recorded shall be checked for readability at least once per year.

5.6 Key Renewal

(1) CA Keys

CA key pairs shall be renewed within 17 years. However, this does not apply if the CA was eliminated before the expiration date of the public key and private key. Notice of renewal of CA key pairs shall be given to subscribers at least one and a half year prior to the implementation of such renewal.

5.7 Recovery from Key Compromise or Disaster

5.7.1 Procedure in Case of Accident and/or Compromise

The Application CA G3 (Root) shall establish a procedure for responding to an accident and/or compromise including the following, so that normal operation can be resumed immediately in case of any such accident and/or compromise.

- Damage to or failure of the hardware, software, data, etc.
- Compromise of a CA private key
- Disaster such as fire or earthquake

5.7.2 Procedure for Recovery from Destruction of Hardware, Software, or Data

If hardware, software, or data is destroyed, recovery work shall be quickly done using hardware, software, and data prepared for backup. Software and data required in a recovery shall be periodically acquired as necessary.

5.7.3 Recovery Procedure if a Private Key Was Compromised

If a subscriber discovers a compromise of a CA private key, the subscriber shall immediately report it to the organization specified in *4.9.3 Revocation Request Procedure* of this CP/CPS.

If Certification Authority operation staff discover compromise of a CA private key, they shall quickly report to the Certification Authority Chief via the Certification Authority System Chief, halt certificate work based on prescribed procedures, and follow the procedures below.

- Revocation of subordinate CA certificates
- Disposal and recreation of CA private keys
- Reissuance of subordinate CA certificates

Also, if the private key of a subordinate CA certificate is compromised, the certificate shall be revoked according to the procedure specified in *4.9 Revocation and Temporary Suspension of Certificates* of this CP/CPS.

5.7.4 Continuity of Operation after Disaster

If an Application CA G3 (Root)'s facility is damaged due to disaster etc., operation shall be performed at a backup site using backup data. Work policies during disasters shall be as follows.

- Highest priority shall be given to publication of CRL via the repositories and web server, with such publication restarted within 48 hours after its halt.
- Work for revocation of subordinate CA certificates shall be resumed within 14 days of the cessation of the work.
- Work for the issuance of subordinate CA certificates shall be resumed after ensuring the complete recovery of the equipment and the security of the Application CA G3 (Root) at the main site.

5.8 Termination of Certificate Operations

The termination of certificate operations shall be decided by the J-LIS. The J-LIS shall notify subscribers and relying parties of the following matters no less than 90 days before the termination of the operations.

- The fact that operations terminated
- Storage organization and disclosure methods for backup data and archive data etc. of the Application CA G3 (Root)'s backup after operations terminate.

Prescribed work termination procedures shall be followed after notification.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

(1) CA Keys

CA key pairs shall be generated by multiple Keys Managers using the HSM for which settings equivalent to FIPS140-2 level 3 have been made.

6.1.2 Distribution of Private Keys to Subscribers

The Application CA G3 (Root) shall not distribute private keys to subscribers.

6.1.3 Distribution of Public Keys to Certification Authorities

Not specified.

6.1.4 Distribution of CA Public Keys to Relying Parties

Self-signed certificates of the Application CA G3 (Root) shall be distributed through, for example, the web server for local governments and the public web server specified in *(2)* of *2.2 Announcement of Information on Certificates* of this CP/CPS.

Distributed self-signed certificates of an Application CA G3 (Root) shall be confirmed by its fingerprint disclosed via the web server which distributed the self-signed certificate. The CA's self-signed certificate and fingerprint shall be disclosed using SSL communication.

6.1.5 Size of Keys

(1) CA Keys

RSA2048 bit length keys shall be used.

(2) Subscriber Keys

RSA1024 bit length keys shall be used.

6.1.6 Generation and Quality Verification of Public Key Parameters

Not specified.

6.1.7 Uses of Keys

Keys shall not be used other than for the following purposes.

(1) CA Keys

CA private keys shall be used in electronic signatures.

6.1.8 Key Lengths Review

Review of key lengths shall be performed at least once per year to decide appropriate period of using CA key pairs and the results of the review shall be documented and stored.

6.2 Protection of Private Keys and Management of Encryption Module Technologies

6.2.1 Standard for and Management of Encryption Modules

(1) CA Keys

CA private keys shall be protected by the HSM for which settings equivalent to FIPS140-2 level 3 have been made.

6.2.2 Control of Private Keys by Multiple People

CA private keys shall be controlled and managed through consultation of multiple Keys Managers

6.2.3 Deposits of Private Keys

Private keys shall not be deposited.

6.2.4 Private Key Backup

Backups of CA private keys shall be done by multiple Keys Managers. CA private keys backed up from an HSM shall be stored in the backup media in an encrypted state. The backup media shall be securely stored by multiple Keys Managers.

6.2.5 Archive of Private Keys

There shall be no archive of private keys.

6.2.6 Transfer of Private Keys to or from Encryption Modules

Not specified.

6.2.7 Storage of Private Keys in Encryption Modules

(1) CA Keys

CA private keys shall be generated in the HSM by multiple Keys Managers, and stored.

6.2.8 Private Key Activation Methods

(1) CA Keys

CA private keys shall be activated by multiple Keys Managers using a Control Key and PIN.

6.2.9 Private Key Deactivation Methods

(1) CA Keys

CA private keys shall be deactivated by multiple IA Operators halting the IA system's services.

6.2.10 Private Key Destruction Method

(1) CA Keys

Disposal of CA private keys in an HSM shall be done by initialization of the HSM by multiple Keys Managers. Also, disposal of CA private keys in backup media shall be done by initialization of the backup media by multiple Keys Managers.

If an HSM is carried out of the room, multiple Keys Managers shall initialize the HSM. Also, if a backup media of CA private keys to be disposed is carried out of the room, multiple Keys Managers shall initialize the CA private key backup media.

6.2.11 Evaluation of Encryption Modules

Specified in *6.1.1 Key Pair Generation* and *6.2.1 Standard for and Management of Encryption Modules* of this CP/CPS.

6.3 Other Methods for Management of Key Pairs

6.3.1 Public Key Storage

Public keys shall be included in the archive of certificates, and stored for the period specified in *5.5.2 Storage Period of Archive Data* of this CP/CPS.

6.3.2 Usage Period of Public Keys and Private Keys

(1) CA Keys

The validity period of the public keys and private keys of the Application CA G3 (Root) shall be up to 20 years of the date on which the public keys and the private keys are validated. However, this shall not apply if the CA is eliminated during the effective period of the public keys and private keys.

If the security of encryption is judged to have become vulnerable, appropriate measures shall possibly be taken at that moment, such as change of key length or algorithm, and key renewal performed.

6.4 Activation Data

6.4.1 Generation and Installation of Activation Data

(1) CA Keys

Operation of HSM which store CA private keys shall be done by multiple Keys Managers and a PIN. The PIN shall be set by a Keys Manager.

6.4.2 Protection of Activation Data

(1) CA Keys

Control Keys and PINs required for activation of HSM which store CA private keys shall be securely stored.

6.4.3 Other Aspects of Activation Data

Not specified.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following functions shall be prepared in the CA system: access control, operator identification and authorization, audit log and archive data collection, recovery of CA keys and system, etc.

6.5.2 Computer Security Evaluation

A system shall be established for objective audits of the situation of execution of security measures and operation management, and computer security evaluation shall be done.

6.6 Life Cycle Technical Controls

6.6.1 System Development

Development, revisions, and changes to a CA system shall be done by a reliable organization in a reliable environment, based on prescribed procedures. A system which has been developed, revised, or changed shall be verified in a CA system evaluation environment, and introduced after obtaining approval by the Certification Authority System Chief. Also, a system specification and verification report shall be documented and stored.

6.6.2 Security Management

In order to maintain and manage the CA system, review and check of the following items shall be done periodically, and the verification results shall be documented and stored.

- Review of security settings for OS (weekly)
- Checking whether to apply modification patches for OS and software (monthly)
- Review of set values for OS and database (quarterly)

6.6.3 Security Evaluation Criteria

Not specified.

6.7 Network Security Controls

For the main site, to prevent improper access, network services which permit access from external networks shall be the minimum required. Also, sufficient security protection measures shall be taken, such as intrusion detection. While operations are being done by the main site, the backup site shall not be connected with an external network.

6.8 Time Stamp

The IA and the RA shall ensure the time synchronization of systems by using a reliable time source and shall provide a time stamp for each record of important information recorded in the systems.

7 Certificate and CRL Profiles

7.1 Certificate Profile

The certificate profile is determined in the Profile Design document.

7.2 CRL Profile

The CRL profile is determined in the Profile Design document.

8 Compliance Audit and Other Evaluation

In order to confirm that certificate work is being performed properly based on this CP/CPS and related rules, compliance audits shall be performed on the Application CA G3 (Root).

8.1 Frequency of Compliance Audits

Compliance audits shall be done periodically, at least once per year. They also may be performed when necessary.

8.2 Auditor Selection and Qualifications

(1) Compliance Audits of the Application CA G3 (Root)

Compliance audits of the Application CA G3 (Root) shall be done by staff that have sufficient knowledge and experience of audit work and certificate work.

8.3 Relations between Auditors and Audit Subjects

Application CA G3 (Root) auditors shall not be people who are involved in work subject to audit.

8.4 Audit Items

Audits by auditors of the Application CA G3 (Root) shall mainly audit whether the Application CA G3 (Root) are properly performing certificate work in compliance with this CP/CPS and related rules, and that suitable measures are being taken against improper conduct from external parties and against internal improper conduct.

8.5 Response to Items Indicated by Audit

The Application CA G3 (Root) shall quickly respond to items indicated by audits as being important or urgent. If there are indications concerning compromise of CA private keys, this shall be prioritized as an emergency situation, and emergency response procedures shall be taken. If there are items indicated by an audit as being important or urgent, during the time until these are improved, operation may be suspended upon the decision of the J-LIS. The J-LIS shall ensure that measures are implemented for the items.

8.6 Notification of Audit Results

Auditors of the Application CA G3 (Root) shall make audit reports when an audit ends. The following items shall be noted in audit reports.

- Dates audit performed
- Summary of audit
- Results of audit

Auditors of the Application CA G3 (Root) shall submit the audit reports to the J-LIS.

Audit reports including audit evidence and improvement measures shall be treated as confidential items, and shall not be disclosed, excluding situations of special provisions due to a contract, etc. Audit reports shall be stored for 5 years.

8.7 Other Verification

To verify whether the certificates issued by the Application CA G3 (Root) satisfy the Baseline requirements, verification shall be implemented on a quarterly basis on 3% sampling of the certificates issued. The results of the verification shall be documented and stored.

9 Other Matters Relating to Operations and Laws

9.1 Fees

Fees concerning use of certificates are separately determined by the J-LIS.

9.2 Responsibilities Concerning Property Rights

The Application CA G3 (Root) shall accept no liability for damage, except in cases involving intentional or gross negligence, when implementing the items specified in *4.5 Use of Key Pairs and Certificates* and *9.6 Representation and Warranty* of this CP/CPS.

9.3 Confidentiality of Information

9.3.1 Confidential Information

The Application CA G3 (Root) shall treat as confidential all information which may cause loss of trust in certification work due to leaks.

9.3.2 Non-confidential Information

Of the information held by the Application CA G3 (Root), items explicitly indicated as announced information, such as certificates and revocation information, shall not be subject to confidential treatment.

9.3.3 Responsibility for Protection of Confidential Information

Classified information shall be retained and managed securely by a specified person responsible for managing data and files that contain such information, in accordance with the related laws and ordinances such as the *Telecommunications Business Law* and the *Act on the Protection of Personal Information*.

Upon receiving an official request for disclosure of confidential information from a law enforcement or a judicial institution by law, or upon receiving a request from a subscriber for the disclosure of confidential information presented by the subscriber to the Application CA G3 (Root), the Application CA G3 (Root) shall disclose the confidential information.

The Application CA G3 (Root) may disclose the classified information specified in *9.3.1 Confidential Information* of this CP/CPS when so required by legal procedures or government administrative procedures.

The Application CA G3 (Root) shall disclose information on the revocation of issued certificates. Details of the reasons for revocation shall not be disclosed.

9.4 Protection of Personal Information

Personal information shall be protected appropriately in accordance with laws such as the *Act on the Protection of Personal Information Held by Administrative Organs* and the *Order for the Enforcement of the Act on the Protection of Personal Information Held by Administrative Organs*.

9.5 Intellectual Property Rights

For key pairs of subordinate CA certificates, regardless of whether they were created by the Application CA G3 (Root) or the subscriber, intellectual property rights shall belong to the subscriber.

For the main party name of a subordinate CA certificate, intellectual property rights shall belong to the subscriber.

Intellectual property rights for the following shall belong to the Application CA G3 (Root): CA key pairs, subordinate CA certificates, CRLs, self-signed certificates and this CP/CPS.

9.6 Representation and Warranty

9.6.1 Representation and Warranty by the Issuing Authority

The Issuing Authority shall represent and warrant the following:

- It appropriately issues, renews, revokes, retains, and announces self-signed certificates and subordinate CA certificates according to this CP/CPS.
- It takes responsibility for the content of issued certificates. (However, the Application CA G3 (Root), which provides an electronic signature for these, does not guarantee their content if signature algorithms are compromised because of, for example, a third party's discovery of a method for falsification or attacking.)
- It performs revocation of certificates and issues a CRL with a validity period of 90 days every 89 days during normal operation.
- It securely manages CA private keys.
- If a CA private key is compromised, it immediately notifies the Certification Authority Chief, and follows the prescribed procedures to implement measures.
- It defines and retains information on certificate profiles to be issued.
- It retains audit logs and archive data concerning the issuance, renewal, and revocation of certificates for the necessary period.
- It retains information on issuance requests, detects any falsification of the issuance information, encrypts confidential information in the IA system, and controls access.
- It always securely monitors the operation of systems in order to ensure stable 24/365 operation.

9.6.2 Representation and Warranty by the Registration Authority

The Registration Authority shall represent and warrant the following:

- It receives requests for the issuance, renewal, and revocation of subordinate CA certificates from the operation directors of the Application CA G3 (Sub), confirms the existence and identity of subscribers, and checks the details of the requests, on the Operation Unit's operating days.
- It makes requests to the Issuing Authority for the issuance and revocation of subordinate CA certificates.

- It notifies the operation directors of the Application CA G3 (Sub) of the completion of the issuance and revocation of subordinate CA certificates.

9.6.3 Representation and Warranty by Subscribers

Subscribers shall represent and warrant their compliance with the matters specified in *4.5.1 Use of Private Keys and Certificates by Subscribers* of this CP/CPS and with the following:

- They make requests for the issuance, renewal, and revocation of subordinate CA certificates based on accurate information.

9.6.4 Representation and Warranty by Relying Parties

Relying parties shall represent and warrant their compliance with the matters specified in *4.5.2 Use of Public Keys and Certificates by Relying Parties* of this CP/CPS.

9.6.5 Representation and Warranty by Other Parties Concerned

Not specified.

9.7 No Warranty

Not specified.

9.8 Restrictions on Responsibility

Scope of the responsibilities arising out of or in relation to the certificate work under this CP/CPS shall be pursuant to laws and statutes of Japan.

9.9 Compensation

Not specified.

9.10 Validity Period and Termination

9.10.1 Validity Period

This CP/CPS shall be validated by the J-LIS's approval.

This CP/CPS shall not be invalidated before the termination specified in *9.10.2 Termination* of this CP/CPS.

9.10.2 Termination

This CP/CPS shall be invalidated at the time of termination of the Application CA G3 (Root), except in those cases specified in *9.10.3 Effects of Termination and Effect Continuation* of this CP/CPS.

9.10.3 Effects of Termination and Effect Continuation

Even if a subscriber terminates the use of a certificate, or even if the operation of the Application CA G3 (Root) is terminated, the provisions of *9.3 Confidentiality of Information*, *9.4 Protection of Personal Information*, *9.5 Intellectual Property Rights*, and *9.14 Applicable Law* of this CP/CPS shall apply to the subscriber, the relying party, and the Application CA G3 (Root), regardless of the reason for termination.

9.11 Separate Notification and Contact between Parties Concerned

The severability clause, remaining provisions clause, entire agreement clause, and notice clause for the Application CA G3 (Root) are as follows.

(1) Severability Clause

Even if any provision of this CP/CPS is invalid or illegal, this will have absolutely no effect on other provisions of this CP/CPS, which shall remain in effect.

(2) Remaining Provisions Clause

Even if a subscriber or a relying party rescinds or cancels an agreement with this CP/CPS, those matters specified in *4.5 Use of Key Pairs and Certificates*, *9.1 Fee*, *9.2 Responsibilities Concerning Property Rights*, *9.3 Confidentiality of Information*, *9.4 Protection of Personal Information*, *9.5 Intellectual Property Rights*, *9.6 Representation and Warranty*, *9.13 Dispute Resolution Procedure*, and *9.14 Applicable Law* of this CP/CPS shall remain valid.

(3) Entire Agreement Clause

This CP/CPS specifies the agreement of the Application CA G3 (Root), subscribers, and relying parties as of the time of agreement. This CP/CPS shall take precedence if the content of this CP/CPS differs from the following items which occurred at or before the time of agreement: The content of discussions between these parties, agreement items, or communications provided from one party to another party such as documents or notices.

(4) Notice Clause

The Operation Unit is the contact point for notices, claims, demands, requests, or other communications to the Application CA G3 (Root) required or permitted by this CP/CPS. The contact point of the Operation Unit is specified in *1.5.2 Contact*.

9.12 Revision

9.12.1 Revision Procedure

The J-LIS shall revise this CP/CPS as necessary.

9.12.2 Notification Method and Period

If the J-LIS revises this CP/CPS, it shall immediately announce the revised CP/CPS. This shall be in the form of a notification to all subscribers and relying parties.

9.12.3 Cases where Object Identifiers Must Be Changed

Not specified.

9.13 Dispute Resolution Procedure

The Application CA G3 (Root), subscribers, and relying parties agree that disputes concerning this CP/CPS shall be finally resolved by the Tokyo District Court, which shall be the court of first instance with exclusive jurisdiction. However, this does not impede petitions for arbitration to the Tokyo Summary Court.

9.14 Applicable Law

Laws, ordinances, and established rules of Japan shall apply to disputes arising from certification work based on this CP/CPS.

9.15 Compliance with Applicable Laws

Not specified.

9.16 Miscellaneous Provisions

Not specified.

9.17 Other Provisions

Not specified.